SQL Server 2000 Security Enhancements

Richard Waymire

Enterprise Program Manager

SQL Server

Microsoft Corp

rwaymi@microsoft.com

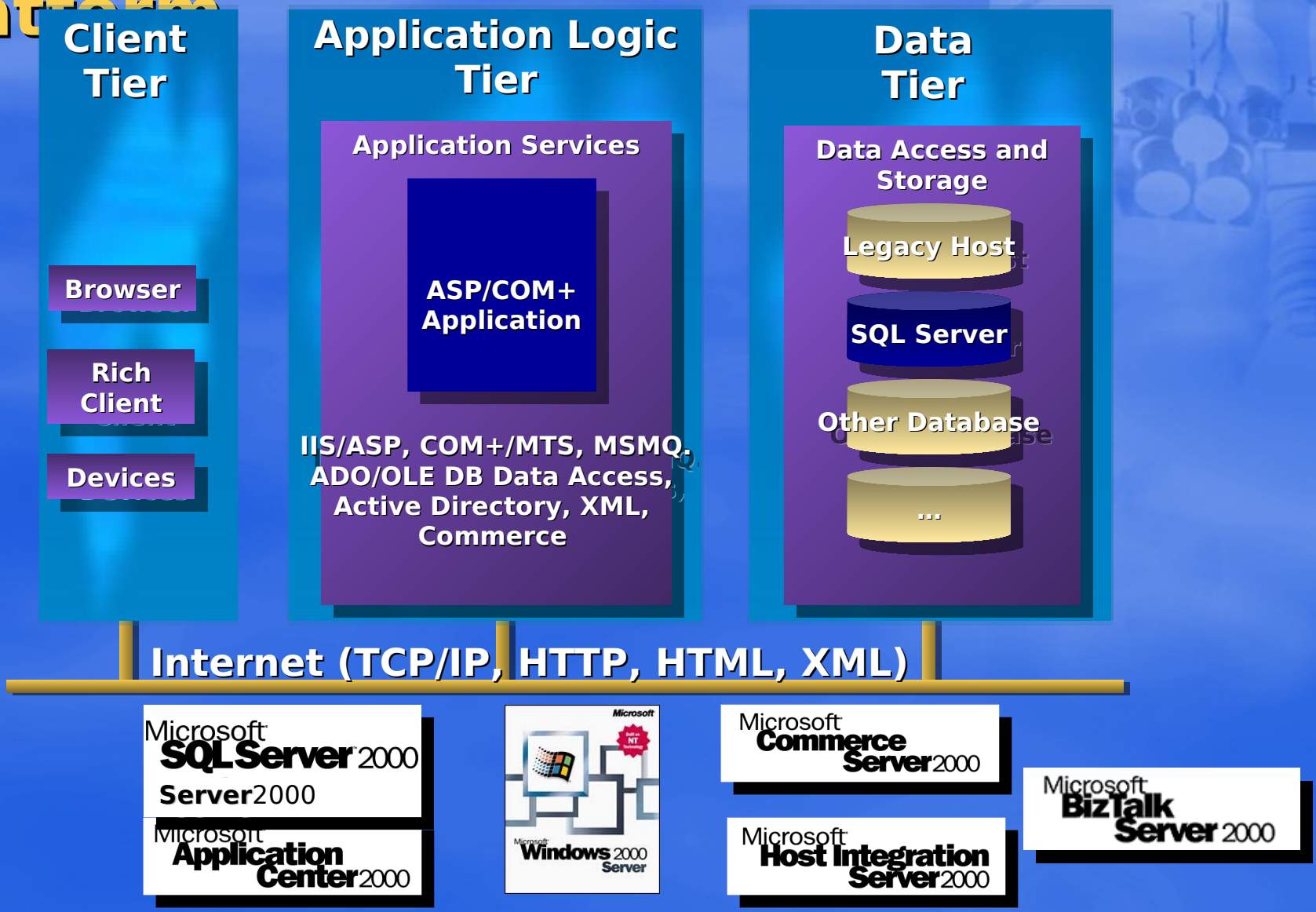

POWER UP
Windows DNA 2000
Readiness Conference
featuring SQL Server 2000

Agenda

- Quick review of 7.0 security
- Security auditing enhancements
- Setup enhancements for security
- Networking improvements
- Server role enhancements
- Misc other enhancements
- SQL server 2000 C2 security evaluation

Windows DNA 2000

Next Generation Web Application Platform



Agenda

- **Quick review of 7.0 security**
- **Security auditing enhancements**
- **Setup enhancements for security**
- **Networking improvements**
- **Server role enhancements**
- **Misc other enhancements**
- **SQL server 2000 C2 security evaluation**

SQL Server Security Model

Network Connection Request / Pre-login Handshake

Connect to the SQL Server Computer

Login Authentication request to SQL Server

Establish Login Credentials

Switch to a database and Authorize access

Establish a Database Context

Attempt to perform some action

Verify permissions for all actions within a database

SQL Server Security Modes

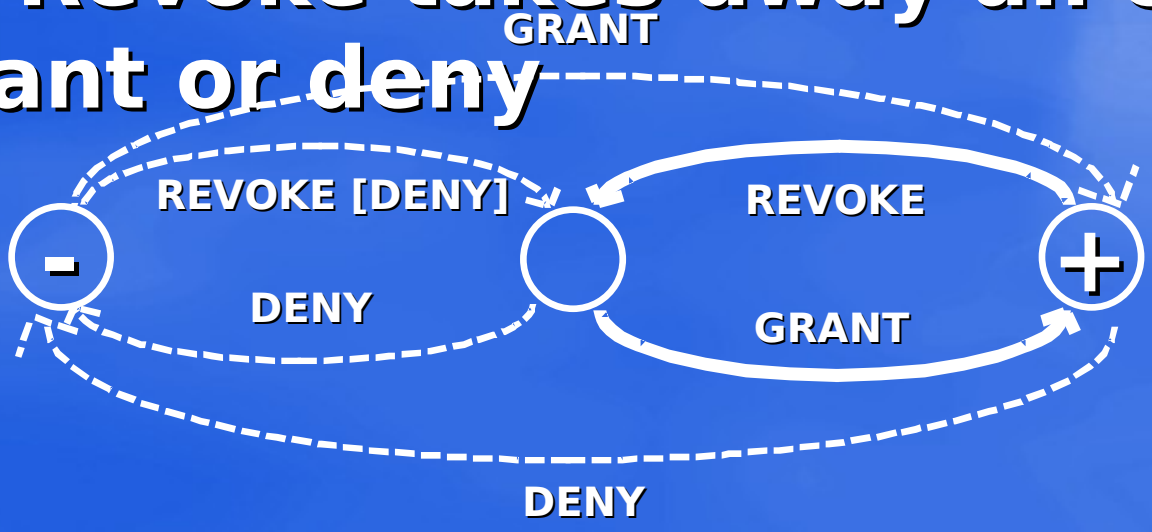
- Integrated security mode
  - Only accept logins using Windows NT/ Windows 2000 credentials
  - Implements network-wide single sign-on
- Mixed security mode
  - Allows integrated logins
  - Allows SQL server based security
  - More difficult to secure

SQL Server Roles

- Fixed server roles
  - Flexible server administration
- Fixed database roles
  - Flexible database administration
- Flexible database roles
  - Custom security combinations
- Application roles
  - Assign rights to applications instead of users

Permissions

- SQL Server three permission verbs:
  - Grant gives a right
  - Deny explicitly denies a right
  - Revoke takes away an existing grant or deny



Agenda

- Quick review of 7.0 security
- **Security auditing enhancements**
- Setup enhancements for security
- Networking improvements
- Server role enhancements
- Misc other enhancements
- SQL server 2000 C2 security evaluation

SQL Server 7.0 Auditing

- SQL server 7.0 audited successful/failed logins
  - Recorded entries in event viewer
    - 18453 :
      login succeeded for user 'REDMOND\rwaymi'. Connection: trusted
    - 18456 :
      login failed for user 'richard'
  - Configured via enterprise manager – server security tab (registry key)

SQL Server 7.0 Auditing (cont)…

- Profiler can also be used to capture SQL Statements
  - Performance overhead can be high
  - Don’t necessarily capture “denied” events
  - No guarantee of 100% audit capabilities
- Why? It was never designed as an auditing mechanism…
  - Built as a performance

SQL Server 2000 Auditing

- We decided that the profiler mechanism was a good one.
- Broke profiler into two separate components:
  - SQL trace – the server side of profiling
  - SQL profiler – the UI components
- New, redesigned implementation of SQL trace for SQL server 2000

SQL Trace Enhancements

- We support file rollover
  - So you can back up the old trace files while a new one is being populated
- You can specify a max file size limit or an end time for a trace
- A “black box” option exists for support
  - Not really a part of auditing

SQL Server 2000 Audit Events

- We audit 18 different kinds of events.
  - Login/logout
  - GRD - statement perms
  - GRD – object perms
  - Add/drop SQL login
  - GRD NT login rights
  - Modify login property
  - Password change event
  - Add/remove from fixed server role
  - Add/remove database role member
  - Add/drop a database role
  - Change Approle password
  - Statement permission used
  - Object permission used
  - Backup/restore event
  - DBCC command issued

SQL Server 2000 Auditing

- **For each event, many subtypes**
- **Example - GRD object permission:**
  - **Grant**
  - **Revoke**
  - **Deny**
- Success or Failure
- Each event includes (at a minimum):
  - Server Name
  - Date/Time of event
  - Application Name
  - NT Username
  - SPID
  - Host Name
  - Statement Text*

How to Turn on an Audit

- **An audit (except for C2 audit) is just a profiler trace**
- **So, turn on a profiler trace with the new profiler procedures, adding auditing events**
- **Set the trace to start with the server if you want a comprehensive audit**
  - **Wrap the trace setup into a stored procedure**
  - **Enable that stored procedure for**

Enabling an Audit(Code Example)

```
Create proc p_audittrace with
    encryption as
 /* Complex code here – won't fit
    on slide */
Exec sp_trace_create @traceid
    output, 2, n'd:\program files\
    microsoft sql server\mssql\audit\
    myaudit', 500
...
Return
Go
Exec sp_procoption 'p_audittrace',
    'startup', 'on'
```

C2-style Auditing

- Must be on an NTFS partition
- All events audited
- We will shut down the server if we can't write to the audit file
- The file rollover size is fixed at 200MB
- The file goes into your mssql\data directory and is named audit_YYYYMMDDHHMMSS_1
- To enable:
  - Exec sp_configure 'C2 audit mode', 1
    go
    reconfigure
  - Shutdown/restart SQL server

Agenda

- Quick review of 7.0 security
- Security auditing enhancements
- Setup enhancements for security
- Networking improvements
- Server role enhancements
- Misc other enhancements
- SQL server 2000 C2 security evaluation

Setup Is Secure Out of the Box

- If you install into NTFS file system, we secure the directories & files
  - Service accounts and the local administrators group get full control, no other permissions set
- We secure the SQL server registry keys
  - Same permissions as the NTFS files
- We default to integrated security on NT

Agenda

- Quick review of 7.0 security
- Security auditing enhancements
- Setup enhancements for security
- **Networking improvements**
- Server role enhancements
- Misc other enhancements
- SQL server 2000 C2 security evaluation

Networking Improvements

- The netlibs will encrypt via SSL/TLS
  - We will always attempt to encrypt for a standard security login handshake
  - Optionally we can encrypt your entire connection
- Full Support for Kerberos & Delegation
  - Linked Servers can use your real Windows login credentials now…

Setting Up for SSL Encryption Over the Network

- **You must have a server certificate to negotiate SSL encryption, and the client must trust that certificate**
- **Set up the certificate using Microsoft Internet Explorer**
- **Make sure to request the server certificate in the fully-qualified DNS name of your server**

Setting Up for SSL Encryption Over the Network

- We will always attempt to encrypt your standard security login attempt
  - Not necessary for Integrated login attempts
- You can optionally request encryption of all communications from a single client
- Just use the checkbox in the client network utility
- But, if the certificate is not trusted by the client, your connection attempt will fail.

Secure Server Option

- Use to force encryption of all communications with this SQL server
- Turn on encryption via the server network utility
- Any connection attempt which can’t negotiate an SSL session will be rejected
- You MUST have a certificate on the server or no communications of any kind is possible (including

Kerberos and Delegation

- Kerberos is the new security protocol for Windows 2000
  - Much more secure than NTLM
- Provides for delegation, which is…
- The ability to bridge credentials across more than server

Enabling Delegation

- **Must be a Windows 2000 domain, using the Active Directory, and client and server using Kerberos**
  - **This means ALL computers here are Windows 2000**
- **Set the following in the Active Directory:**
  - **The *Account is sensitive and cannot be delegated* option must not be set for the user requesting delegation.**
  - **The *Account is trusted for delegation* option must be set for the service account of SQL Server.**
  - **The Server running SQL Server must be allowed to delegate credentials (the *Computer is trusted for delegation* option)**

Enabling Delegation (User)

- SQL Server must have a Service Principal Name (SPN) assigned by the Windows 2000 account domain administrator assigned to the service account of the SQL Server service on that particular machine
  - Must enable via the setspn utility in the Windows 2000 Resource Kit
  - Setspn –A MSSQLSvc/Host:port serviceaccount
    - Example: setspn –A MSSQLSvc/rwaymi0.redmond.corp.microsoft.com:1433 rwaymi
      - Don’t specify redmond\rwaymi – doesn’t work

Enabling Delegation (machine)

- Or, you can run under the localsystem account and we will self-register at service startup
  - SQL Server automatically registers the SPNs itself – no user action required – one change to Setspn if you wish to use it
  - Setspn –A MSSQLSvc/Host:port machine
    - Example: setspn –A MSSQLSvc/rwaymi0:1433 rwaymi0
- LocalSystem is much easier – but you lose other functionality

More delegation stuff…

- All accounts must be in the same domain or within the same trust tree.
- Don’t use dynamic tcp ports for named instances
  - Part of the SPN is the port number
- Your better get along with your domain administrators if you want this to work ☺

Agenda

- Quick review of 7.0 security
- Security auditing enhancements
- Setup enhancements for security
- Networking improvements
- Server role enhancements
- Misc other enhancements
- SQL server 2000 C2 security evaluation

Fixed Server Role Enhancements

- **BulkAdmin fixed server role has been added**
  - **Allows you to use the BULK INSERT statement**
  - **You still need insert rights to the table you're loading**
- **SecurityAdmin can change passwords**
  - **Except for sysadmin role members**
- **ServerAdmin can control all aspects of messages**
  - **Implementation wasn't clean in SQL server 7.0**
  - **Now you can run sp_addmessage, sp_dropmessage, and**

Agenda

- Quick review of 7.0 security
- Security auditing enhancements
- Setup enhancements for security
- Networking improvements
- Server role enhancements
- Misc other enhancements
- SQL server 2000 C2 security evaluation

Misc. Security Enhancements

- **Full support for using the Windows 2000 encrypted file system (EFS)**
- **Enhancements to server based encryption**
  - **Using the crypto API for encryption of misc. Objects/passwords in SQL server**
- **Eliminated the SUID column from all system tables**
  - **sysdatabases, syslogins, sysremotelogins, sysusers, and sysprocesses**

Backup Security

- We Password Protect…
  - Backup Media
  - Backup Sets
- Prevents unauthorized restore using our tools
  - Not encrypted…data can be interpreted by another program
- Prevents unauthorized append to media by our tools and other MTF compliant applications
- Does not protect against media overwrite

User-Defined Functions

- To create:
  - New CREATE FUNCTION permission.
  - If SCHEMABOUND: REFERENCES permission on any called function/table/view.
- REFERENCES permission can now be granted to Views and Functions.
- To invoke:
  - EXECUTE permission for scalar functions, SELECT permission for table-valued functions
  - If used in a CHECK constraint or DEFAULT defn., REFERENCES permission on function also needed.
  - See talk 2-308 Transact-SQL

Agenda

- Quick review of 7.0 security
- Security auditing enhancements
- Setup enhancements for security
- Networking improvements
- Server role enhancements
- Misc other enhancements
- SQL server 2000 C2 security evaluation

C2 Security Evaluation

- **SQL server 2000 is undergoing evaluation for C2 security rating**
- **Should be complete shortly after release**
- **Needed auditing to comply with C2**
- **Significantly increased security testing in shiloh**

Summary

- **Security enhancements throughout the product**
- **At completion of setup on a windows NT or windows 2000 system you are secure**
- **Network level security greatly enhanced**
- **Support for several windows 2000 security features enabled**

POWER UP

Microsoft